



Billing Code: 3510-13

## DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: [140321260-4260-01]

National Cybersecurity Center of Excellence (NCCoE) and Financial Services Sector IT  
Asset Management Use Case

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide products and technical expertise to support and demonstrate security platforms for IT asset management for the financial services sector. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the Financial Services sector program. Participation in the use case is open to all interested organizations.

DATES: Interested parties must contact NIST to request a letter of interest. Letters of interest will be accepted on a rolling basis. Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the use case has been completed, NIST will post a notice on the NCCoE financial services program website at [nccoe.nist.gov/financial-services/](http://nccoe.nist.gov/financial-services/) announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

ADDRESSES: The NCCoE is located at 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to [financial\\_NCCoE@nist.gov](mailto:financial_NCCoE@nist.gov); or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Organizations whose letters of interest are accepted in accordance with the Process set forth in the SUPPLEMENTARY INFORMATION section of this notice will be asked to sign a Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: [http://nccoe.nist.gov/The-Center/Get\\_Involved/NCCoE\\_Consortium\\_CRADA\\_Example.pdf](http://nccoe.nist.gov/The-Center/Get_Involved/NCCoE_Consortium_CRADA_Example.pdf).

FOR FURTHER INFORMATION CONTACT: Mike Stone via email at [financial\\_NCCoE@nist.gov](mailto:financial_NCCoE@nist.gov); or telephone 240-314-6813; National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional

details about the NCCoE Financial Services Sector program are available at <http://nccoe.nist.gov/financial-services>.

#### SUPPLEMENTARY INFORMATION:

**Background:** The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

**Process:** NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for IT asset management for the financial services sector. Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a letter of interest, which the party must complete, certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the use case objective or requirements

identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this use case. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST. NIST published a notice in the Federal Register on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships; (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

**Use Case Objective:** To effectively manage, utilize and secure an asset, you first need to know the asset's location and function. While many financial sector companies label physical assets with bar codes and track them with a database, this approach does not answer questions such as, "What operating systems are our laptops running?" and "Which devices are vulnerable to the latest threat?" The goal of this project is to provide answers to questions like these by tying existing data systems for physical assets and security and IT security and support into a comprehensive IT asset management (ITAM) system. In addition, financial services companies can employ this ITAM system to dynamically apply business and security rules to better utilize information assets and protect enterprise systems and data. In short, this ITAM system will give companies the ability to track, manage and report on an information asset throughout its entire life cycle.

**Requirements:**

Each responding organization's letter of interest should identify which security platform components or capabilities it is offering. Components are listed in section six of the IT Asset Management for Financial Services use case and include, but are not limited to:

1. physical asset management systems/databases
2. physical security management systems/databases
3. multiple virtual testing networks and systems simulating receiving, security, IT support, network security, development and sales departments
4. physical access controls with standard network interfaces

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section two of the IT Asset Management for Financial Services use case:

1. be capable of interfacing with multiple existing systems
2. complement existing asset management, security and network systems
3. provide APIs for communicating with other security devices and systems such as firewalls and intrusion detection and identity and access management (IDAM) systems
4. know and control which assets, both virtual and physical, are connected to the enterprise network
5. provide fine-grain asset accountability supporting the idea of data as an asset
6. automatically detect and alert when unauthorized devices attempt to access the network, also known as asset discovery
7. integrate with ways to validate a trusted network connection
8. enable administrators to define and control the hardware and software that can be connected to the corporate environment
9. enforce software restriction policies relating to what software is allowed to run in the corporate environment
10. record and track the prescribed attributes of assets
11. audit and monitor changes in the asset's state and connection
12. integrate with log analysis tools to collect and store audited information

Responding organizations need to understand and, in their letters of interest, commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components
2. Support for development and demonstration of the IT Asset Management for the Financial Services Sector use case in NCCoE facilities which will be conducted in a manner consistent with Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63)

Additional details about the IT Asset Management for the Financial Services sector Use Case are available at <http://nccoe.nist.gov/financial-services>.

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the consortium agreement in the development of the IT Asset Management for Financial Services capability. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each prospective participant will train NIST personnel as necessary, to operate its product in capability demonstrations to the healthcare community. Following successful demonstrations, NIST will publish a description of the security platform and its performance

characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the IT Asset Management for Financial Services Use Case. These descriptions will be public information.

Under the terms of the consortium agreement, NIST will support development of interfaces among participants' products, including IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of the IT Asset Management for Financial Services capability will be announced on the NCCoE Web site at least two weeks in advance at <http://nccoe.nist.gov/>. The expected outcome of the demonstration is to improve IT asset management across an entire financial services enterprise. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE Web site <http://nccoe.nist.gov/>.

Dated: May 1, 2014

Kevin A. Kimball  
Chief of Staff

[FR Doc. 2014-10349 Filed 05/05/2014 at 8:45 am; Publication Date: 05/06/2014]